AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ryan S. Burke, depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since October 2012. I am currently assigned to the FBI's New Hampshire Major Offender Task Force ("MOTF") where I am tasked with investigating violent criminals, gang members, and significant drug traffickers throughout the state. As part of the MOTF, I work alongside law enforcement officers from various local, state, and federal agencies throughout the state of New Hampshire. I am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

2. Throughout my career, I have led and/or been involved with investigations of drug distribution, violent crimes, and other offenses. My investigations have included the use of the following investigative techniques: physical surveillance; handling of cooperating sources and witnesses; exploitation of cellular, social media, and Internet Protocol ("IP") based communications data; execution of search and seizure warrants; wire and electronic interception of communications; and the execution of arrest warrants. Based on my training, experience, and information provided to me by other law enforcement officers, I am familiar with the modus operandi used by individuals engaged in the commission of various criminal offenses, including the unlawful distribution of controlled substances.

PURPOSE OF AFFIDAVIT

3. I submit this affidavit in support of applications for warrants to search the following:

a. A dark blue Mercedes CLK 500 sedan with New Hampshire license plate 4462091 and according to NHDMV bearing Vehicle Identification Number WDBTJ75J13F058915 (hereafter, "**Target Vehicle**"); and

b. A black iPhone in a tie-dye case which was seized from Matthew Schnell on March 22, 2023 in Concord, New Hampshire (hereafter, "**Target Device**").

4. Based on the information contained herein, there is probable cause to believe that the **Target Vehicle** and **Target Device**, described in Attachments A-1 and A-2 respectively, contain evidence, fruits, and/or instrumentalities of the crimes of distribution of controlled substances, and conspiracy to do same (21 U.S.C. §§ 841, 846); and illegal use of a communication facility (21 U.S.C. § 843(b)), described in Attachments B-1 and B-2 respectively.

5. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, and information received from other law enforcement officers. I have not set forth every detail I or other law enforcement officers know about this investigation but have set forth facts that I believe are sufficient to evaluate probable cause as it relates to the issuance of the requested warrants.

INVESTIGATION BACKGROUND

6. Since approximately October 2022, the FBI and New Hampshire State Police ("NHSP") have been investigating Matthew Schnell, Thomas Conway, Michael Raiche, and other individuals who are understood to be participants in a conspiracy to distribute controlled substances in New Hampshire and elsewhere. To date, fourteen controlled purchases of an approximate aggregate amount of 2.5 pounds of methamphetamine and 250 grams of fentanyl have been facilitated through Conway and/or Raiche. On March 7, 2023, law enforcement initiated wire and electronic interceptions over Conway's cellular phone ("TT-1") pursuant to an order issued by United States District Judge Samantha Elliott (District of New Hampshire). Based on

information described below, investigators believe Schnell to be a methamphetamine supplier to Conway and believe evidence of that relationship is present within the **Target Vehicle** and on the **Target Device**.

PROBABLE CAUSE

7. In approximately July 2020, Schnell was interviewed by Drug Enforcement Administration ("DEA") investigators and admitted to being a distributor of controlled substances. Further, Schnell informed the DEA that he had previously smuggled controlled substances through airport baggage screening and onto domestic flights.

8. On November 7, 2022, at approximately 11:40 a.m., at the direction of law enforcement, a Cooperating Witness ("CW-1")[1] called Conway while in the presence of law enforcement to arrange the purchase of four ounces of methamphetamine. Conway directed CW-1 to contact "Mike" – a reference to Michael Raiche. CW-1 then texted Raiche at 603-851-1910 beginning at approximately 11:48 a.m. and Raiche agreed to sell the methamphetamine to CW-1. Raiche directed CW-1 to 8 Country Club Drive, Apartment 2, in Manchester, New Hampshire.

[1] CW-1 has been cooperating with law enforcement since approximately October 2022. Prior to agreeing to cooperate with law enforcement, CW-1 was arrested for possession of methamphetamine and is motivated to work with law enforcement solely in hopes of consideration in that case. CW-1 has not received any monetary payments. Since becoming a cooperating witness, CW-1 has not, to the knowledge of law enforcement, utilized controlled substances, nor has CW-1 conducted any purchases of controlled substances without law enforcement direction. CW-1 has been arrested for the following offenses: Driving After Suspension [M] (NH RSA 263:64), False Report to Law Enforcement [M] (NH RSA 641:4, I), Burglary [M] (NH RSA 635:1, V), Transporting Drugs [M] (NH RSA 265-A:43), Possession of Controlled Drug [F] (NH RSA 318-B:2,I), Disobeying an Officer [M] (NH RSA 265:4), Resisting Arrest [M] (NH RSA 642:2), Identity Fraud [F] (NH RSA 638:26,I(A)), Felon in Possession of a Dangerous Weapon [F] (NH RSA 159:3), Violation of Probation [M] (NH RSA 504-A:4), Receiving Stolen Property [M] (NH RSA 637:7), Simple Assault [V] (NH RSA 631:2-a), Sale of a Controlled Drug [F] (NH RSA 318-B:2,I), Theft Willful Concealment [M] (NH RSA 637:3-a,II), Theft by Unauthorized Taking [M] (NH RSA 637:3). CW-1 has not been convicted of all the previously mentioned charges and most have been declined for prosecution. CW-1 has provided information related to criminal activity which has been corroborated by law enforcement. For example, when CW-1 first agreed to cooperate, CW-1 identified Conway and described Conway's pattern of behavior related to drug trafficking, which was consistent with evidence later developed in this investigation and described herein.

CW-1 was followed by law enforcement to 8 Country Club Drive. Upon arrival, CW-1 exited his/her vehicle and entered Apartment 2. Investigators observed the **Target Vehicle** in the apartment's parking lot. While inside, CW-1 paid Raiche $1,600 for four ounces of methamphetamine. During their conversation, Raiche could be heard referring to someone as "boss man" – what I believe was a reference to Conway. CW-1 then exited the apartment and was followed by law enforcement to a pre-determined location where CW-1 provided the substance to law enforcement.[2] The substance was tested with a TruNarc portable chemical analyzer and tested positive for methamphetamine.

9. On November 22, 2022, CW-1 called Conway to purchase methamphetamine. Conway stated he was going to send Raiche to meet CW-1. Investigators located the **Target Vehicle** at the Irving Gas Station in Bow, just down the street from the agreed meet spot of the Tru by Hilton parking lot in Concord. Investigators observed the **Target Vehicle** depart from Irving to the Tru by Hilton parking lot. Investigators then observed Raiche exit the vehicle and enter CW-1's vehicle. CW-1 successfully bought four ounces of methamphetamine from Raiche. Investigators followed the **Target Vehicle** to another address in Concord before following it to a storage facility in Chelmsford, MA.

10. On December 15, 2022, CW-1 called Conway to purchase methamphetamine in Concord at the Tru by Hilton parking lot. Investigators observed the **Target Vehicle** occupied by three individuals pull into the Tru by Hilton parking lot. Conway was observed exiting the **Target Vehicle** and entering CW-1's vehicle. After selling four ounces of methamphetamine to CW-1,

[2] For all of the controlled purchases described herein, a set of standard protocols was employed to ensure the evidentiary reliability of the purchase. CW-1 was searched prior to the purchase to ensure that CW-1 had only the necessary buy money and no pre-existing drugs. CW-1 was provided a concealed audio recorder to record the transaction. CW-1 was followed away from the location to a pre-determined location, where the substance purchased was immediately turned over to law enforcement.

Conway exited the vehicle and re-entered the **Target Vehicle**. The **Target Vehicle** then departed the lot and investigators followed the CW-1 to a pre-determined location where the suspected methamphetamine was collected from CW-1.

11. On January 18, 2023, CW-1 texted Conway to purchase methamphetamine in Concord at the Tru by Hilton parking lot. Investigators observed Conway driving the **Target Vehicle**. Once in the lot, Conway exited the **Target Vehicle** and entered CW-1's vehicle where Conway sold CW-1 three ounces of methamphetamine. Conway then exited CW-1's vehicle and re-entered the **Target Vehicle**. The **Target Vehicle** then departed to another address in Concord and investigators followed the CW-1 to a pre-determined location where the suspected methamphetamine was collected from CW-1.

12. On February 15, 2023, investigators directed CW-1 to contact Conway to request to purchase methamphetamine. During the recorded call, CW-1 asked Conway if he/she could meet with Conway in Concord to purchase methamphetamine. Conway informed CW-1 he only had three ounces. On a subsequent call to Conway, he told CW-1 that it wouldn't be "worth the trip" because it was only "two." Conway then told CW-1 that he would be driving to his "plug's house" to get more – a statement I believe meant that Conway intended to obtain more methamphetamine from Schnell. Ultimately, CW-1 did not conduct another deal with Conway until February 22, 2023.

13. On February 22, 2023, a GPS tracking device installed on Conway's Volkswagen Jetta pursuant to a warrant authorized by United States Magistrate Judge Andrea K. Johnstone (District of New Hampshire) reported locations consistent with travel by the Jetta to Logan International Airport in Boston, Massachusetts. According to the data collected, the vehicle arrived at the airport at approximately 6:00 p.m. and departed shortly after. The vehicle traveled north

from the airport without stopping (besides at intersections presumably because of traffic lights) until it exited I-93 in Stoneham, Massachusetts, where it was met by surveillance units at a gas station. At the gas station, investigators observed Conway and Schnell in the Jetta. After a brief stop at the gas station, Conway and Schnell inside the Jetta returned to the highway and traveled north without stopping until their arrival at the Tilton House of Pizza in Tilton, New Hampshire.

14. Conway and CW-1 had previously agreed to conduct a methamphetamine transaction in Concord, New Hampshire on February 22, 2023. However, while Conway and Schnell were in transit between the airport and Tilton, Conway requested CW-1 instead meet him at the Tilton House of Pizza. CW-1 was followed to the pizza shop while other surveillance units continued to follow Conway and Schnell northbound. Upon arrival, CW-1 parked next to Conway's Jetta. Schnell was observed by investigators entering the pizza shop and then returning to the Jetta with food. Conway and Schnell then departed from the pizza shop as CW-1 remained in place. Conway then sent a text message to CW-1 stating, "I've got to go do [sic] someone off and I'll be right back… Just got to weigh it out. What kind of time constrain [sic] are you working with? Do you have to be home at a certain time?"

15. Investigators followed Conway and Schnell to an address in Franklin, New Hampshire where Schnell was dropped off. Schnell was observed carrying luggage and food from the pizza shop into a residence. Conway then returned to the pizza shop and sold three ounces of suspected methamphetamine to CW-1. During their meeting, Conway informed CW-1, "I went five days without having anything" – which I believe was a reference to having been without methamphetamine. Based on the attempted controlled purchase on February 15, 2023, the facts leading up to the completed deal on February 22, 2023, and Schnell's previous admissions to DEA, I believe Conway picked Schnell up from the airport after Schnell had arrived on a flight on which

he had smuggled methamphetamine. This would also explain why Conway informed CW-1 he would need to "weigh it out" after departing the pizza shop where CW-1 was also parked.

16. On March 10, 2023, United States Magistrate Judge Andrea K. Johnstone (District of New Hampshire) authorized a warrant to compel Verizon Wireless to provide the FBI with prospective and historical location data for one of Schnell's cellular phones (401-871-6901 / "TT-6901"). A review of the historical data, which covered the previous thirty days from the date the warrant was issued, provided some detail on Schnell's travels prior to returning to Logan International Airport on February 22, 2023. The following timeline outlines Schnell's travel based on the cellular towers utilized by his device:

a. February 19, 2023, 8:20 p.m. to 8:48 p.m. (Eastern): TT-6901 connects to cellular towers at Logan International Airport.
b. February 20, 2023, 1:03 a.m. (Pacific): TT-6901 connects to a cellular tower at Los Angeles International Airport.
c. February 20, 2023, 4:18 a.m. (Pacific): TT-6901 begins connecting to cellular towers in vicinity of the Canoga Park neighborhood of Los Angeles.
d. February 20, 2023, 11:30 p.m. (Pacific): TT-6901 connects to a cellular tower at Los Angeles International Airport.
e. February 21, 2023, 12:09 a.m. (Pacific): TT-6901 connects to a cellular tower at Los Angeles International Airport.
f. February 22, 2023, 12:39 p.m. (Eastern): TT-6901 connects to a cellular tower at Hartsfield-Jackson Atlanta International Airport.
g. February 22, 2023, 5:02 p.m. to 6:00 p.m. (Eastern): TT-6901 connects to cellular towers at Logan International Airport.
h. TT-6901 then travels north into New Hampshire.

17. As previously stated, on March 7, 2023 investigators initiated interceptions of wire and electronic communications over TT-1 – Conway's cellular phone. To date, numerous voice calls and text messages exchanged between Conway and Schnell, using TT-1 and TT-6901 respectively, have been intercepted. Additionally, investigators have intercepted conversations between Conway and Schnell using TT-1 and 310-409-8148 ("TT-8148") respectively. To date, there have been approximately 77 pertinent voice calls and text messages between TT-1 and both

of Schnell's phones. Based on my training and experience, the totality of all the conversations intercepted over TT-1 have confirmed that Schnell supplies Conway with methamphetamine.

18. The conversations between Conway and Schnell, at times, have included explicit references to thousands of dollars and references to quantities which I believe are pounds of methamphetamine. However, much of what Schnell has told Conway over the wiretap has been independently determined by investigators to be fictitious. For example, Schnell has lied to Conway about his whereabouts on numerous occasions and has repeatedly promised that he would re-supply Conway by a certain date and time, but failed to do so. Their conversations have included references to Schnell travelling to unspecified places which I believe are understood by Conway to be outside of New England. Schnell has also repeatedly referenced lost baggage at the airport. While I know based on my training and experience that drug suppliers may lie to their customers, it should be noted that Schnell has lied to Conway more than what would be expected in a normal supplier-customer relationship.

19. On March 20, 2023 at approximately 5:24 p.m., TT-1 made an outgoing call to TT-8148. During the call, Schnell informed Conway that he was at the airport and indicated that "these people" – an apparent reference to airline employees – did not know where "it's at' – an apparent reference to a lost bag. The location data for TT-6901 confirmed Schnell's phone was at an airport. However, Schnell failed to mention to Conway that he had just landed at Philadelphia International Airport from a flight that originated at Logan International Airport.

20. On March 20, 2023 at 9:15 p.m. (Pacific), TT-6901's location data indicated the phone had arrived at Los Angeles International Airport. After departing the airport, TT-6901 traveled again to the Canoga Park neighborhood of Los Angeles where it stayed for approximately one hour. By March 21, 2023 at approximately 5:00 a.m. (Pacific), TT-6901 remained in the

vicinity of Los Angeles International Airport until approximately March 22, 2023 at 1:29 a.m. (Pacific). Its next reported location was at Logan International Airport on March 22, 2023 at 9:15 a.m. (Eastern) – consistent with JetBlue flight 988 from LAX to BOS which was temporarily delayed but departed from LAX at 1:20 a.m. (Pacific) and arrived in BOS at 9:09 a.m. (Eastern).

21. Based on all of the aforementioned and specifically the fact that Conway was out of methamphetamine seemingly until he picked up Schnell at Logan International Airport following his February 19-22, 2023 trip to Los Angeles, I believe Schnell likely obtained methamphetamine again while in Los Angeles during this March 20-22, 2023 trip. Additionally, as detailed below, Schnell was expected to depart the airport in the **Target Vehicle**, which investigators knew had been used in the past to facilitate the distribution of methamphetamine. Consequently, I believed Schnell would be departing the airport with methamphetamine.

22. Upon Schnell's arrival to Logan International Airport on March 22, surveillance members were located inside the airport and in the vicinity of the **Target Vehicle**, which was located in the airport parking garage. Surveillance was able to observe Schnell exit the secured area of the terminal with two carry-on bags – a dark-colored backpack and a Marshalls shopping bag. Schnell appeared to have difficulty locating his checked baggage and ultimately wandered into the parking garage where he was observed sitting in a stairwell. During that time, at approximately 10:44 a.m., an incoming call was intercepted over TT-1 with TT-8148. The following conversation took place between Conway and Schnell:

- Conway: Hey, what's up? Hey, what's up?
- Schnell: What are you doing?
- Conway: Just laying around. I got a meeting at 12:30.
- Schnell: About what
- Conway: Narcotics anonymous
- Schnell: What
- Conway: Narcotics anonymous. Some stuff I'm doing for my court thing

- Schnell: Speaking of…. *sigh* I need to get out of where I am and I'll talk to you, but anyways you have $50 on CashApp
- Conway: I don't have $50 on CashApp
- Schnell: Fuck. Its not good.. *sigh* ughhhhhhhh
- Conway: I gave my last $15 like twenty minutes ago
- Schnell: That's cool. That's not what I'm bugging about. I can figure that out. Stay tuned though. It's not good things I think
- Conway: What? What do you think?
- Schnell: Ugh, I'll talk to you. You'll probably see me after that meting

23. I believe the above-conversation illustrated concern by Schnell regarding his missing baggage, potentially concerned about someone discovering controlled substances inside it. Schnell eventually re-entered the airport and located his suitcase at the JetBlue baggage office. He was then observed loading his three bags into the **Target Vehicle** and eventually departed Logan International Airport alone in the **Target Vehicle**. Surveillance units followed him out of the airport and observed him at a gas station moving items around the inside of the **Target Vehicle** for some time. Schnell then departed the gas station and surveillance units lost him temporarily but quickly re-established surveillance on Schnell in the **Target Vehicle** northbound on I-93 in Massachusetts.

24. Schnell in the **Target Vehicle** was followed through New Hampshire on I-93 until he was eventually stopped in Concord at approximately 2:31 p.m. by NHSP at the request of investigators who knew Schnell to have an active arrest warrant. The Trooper told Schnell that he had been stopped for following too close to another vehicle. When asked, Schnell stated he was coming from New Bedford, Massachusetts. Upon request for identification, Schnell admitted that he was not permitted to drive. Schnell was arrested without incident. The **Target Device** was located and removed from his pocket.

25. At approximately 3:45 p.m., investigators spoke with Schnell at the NHSP barracks interview room in Concord. Schnell was read his Miranda Rights and signed a form acknowledging that they were read to him. Schnell also agreed to a consensually recorded conversation. Over the

course of the conversation, Schnell stated that he primarily lives in Las Vegas, Nevada with his sister. Schnell claimed to do contract work as a fiberoptic installer for friends as he stated it was hard to get work without being in a union and because of his status as a convicted felon. Schnell claimed that he would travel to Los Angeles, California to work for a friend who has contract work and another friend who has labor work.

26. Over the course of the conversation, Schnell provided several different itineraries for the last several weeks. The first story was that Schnell traveled from Las Vegas to Massachusetts. Schnell then changed the story moments later to him flying in from Los Angeles. Schnell claimed he was in Los Angeles for three to four days due to having issues after losing his paper ID resulting in him missing several flights. Schnell claimed he went from Las Vegas to Los Angeles to Massachusetts. Schnell would eventually state that he went from Boston to Los Angeles and took a bus to see his sister where he spent one day in Las Vegas, but then changed his story to a friend drove over and took him to Las Vegas and he was gone for ten to eleven days. Investigators know this to be false based on the location data for TT-6901 and surveillance observations of Schnell at his residence in Bellingham, Massachusetts.

27. Eventually, investigators advised Schnell of their knowledge that he flew from Boston to Philadelphia to Los Angeles on March 20, 2023 before arriving back to Boston from Los Angeles earlier in the day. Schnell then stated that he flew out there because he had to move a vehicle he was storing at a friend's apartment. Although Schnell admitted the friend had the keys to the car, Schnell stated that he didn't have the friend move the car because he didn't want the friend to put it on the street. Schnell then stated that he simply left the car on the side of Orville Street "in the valley." Schnell also stated he went out to Los Angeles to work, but upon arrival his

friend no longer had work available. Schnell was unable to provide an explanation as to what changed in the span of less than a day that would result in no work being available.

28. During the conversation, investigators discussed the information that Schnell had previously provided to the DEA. Schnell stated that he has been working legitimately and no longer distributes controlled substances but provided information on how he used to traffic methamphetamine utilizing airlines. Schnell advised that the canines in the domestic terminals are not trained on narcotics and that the TSA doesn't really check for "that" – a reference to controlled substances. Schnell made reference to smuggling drugs inside his neck pillow on several occasions.

29. Schnell admitted that the **Target Vehicle** was a friend of a friend's, but he had been using it for two weeks. Schnell admitted ownership of the luggage in the trunk, as well as a backpack and shopping bag in the backseat. Schnell advised that the items were in their original spots from loading them at Logan Airport. However, investigators observed Schnell at a gas station nearby the airport open the luggage and receive a briefcase from within. Schnell then placed the briefcase onto the front seat. Investigators also believe they observed Schnell moving the luggage from the backseat to the trunk and placing the briefcase into the interior of the vehicle, which is inconsistent with Schnell's statements about their positioning.

30. At the conclusion of the interview, Schnell admitted the **Target Device** was assigned the phone number for TT-8148, which was used by Schnell to communicate with Conway regarding the acquisition of controlled substances. He also admitted to having two other cellular phones that belong to him.

31. I therefore submit that there is probable cause to search both the **Target Vehicle** (and any electronic devices found within it) and the **Target Device** for evidence, fruits, and

instrumntalities of the crimes of distribution of controlled substances, and conspiracy to do same (21 U.S.C. §§ 841, 846); and illegal use of a communication facility (21 U.S.C. § 843(b)).

USE OF CELLULAR PHONES TO FACILITATE CRIMINAL ACTIVITY

32. Based upon training, knowledge, and experience as well as from information obtained from other law enforcement officers, I know that it is common practice for individuals engaged in criminal activity to routinely utilize cellular phones, text messaging apps, social media, and coded communications to interact with and do business with co-conspirators. Further, I know that individuals engaged in criminal activity often use cellular phones to plan and facilitate criminal activity.

33. Therefore, I know that evidence of the crimes listed above can be found in cellular phones similar to the **Target Device**. Such evidence includes, but is not limited to:

a. Names, addresses, telephone numbers, usernames, and email addresses of co-conspirators;

b. Messages/emails sent to or received from co-conspirators or other entities necessary for conducting illegal activity such as arranging travel and transportation;

c. Photographs/videos of themselves and co-conspirators;

d. Photographs/videos of contraband and proceeds of illegal activity;

e. Records of social media and app usage in furtherance of illegal activity;

f. Records of internet activity in furtherance of illegal activity;

g. Calendar entries and to-do lists; and

h. Financial information and bank accounts used in furtherance of illegal activity.

TECHNICAL INFORMATION RELATED TO CELLULAR PHONES

34. Based upon my training, knowledge, and experience, I know that cellular telephones such as the **Target Device** and other devices that may be found in the **Target Vehicle** are capable of storing information including, but not limited to, text and audio communications, call history, contact information, calendar entries, downloads, applications, videos, photographs, and electronic documentation in the cellular telephone's memory. In addition, I know that a forensic examination of a cellular telephone and these other devices can result in the retrieval of such data which has been stored on them, even after the passage of time, because files that have been hidden or deleted can still be recovered.

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other

information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same

capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

36. I know that many smartphones like the **Target Device** and other devices that may be found in the **Target Vehicle** (which are included in Attachment B's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Based on my training, experience, and information provided to me by other law enforcement personnel, I am aware that individuals commonly store records of the type described in Attachment B in mobile phones, computer hardware, computer software, and storage media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described in Attachment B-1 and B-2, these applications seek permission to search for records that might be found in the **Target Vehicle**, and the **Target Device**, in whatever form they are found. One form in which the records might be found is data stored on a computer's

hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

38. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

39. *Probable cause*. I submit that if a computer or storage medium is found in the **Target Vehicle**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

40. *Forensic evidence*. As further described in Attachment B-1 and B-2, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Target Vehicle**, or on the **Target Device**, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial

evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether

data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

41. *Necessity of seizing or copying entire computers or storage media*. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic

electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

42. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

43. Because several people have been observed operating the **Target Vehicle**, it is possible that the **Target Vehicle** will contain storage media that are predominantly used, and perhaps owned, by persons other than Schnell. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

44. I submit that this affidavit supports probable cause for warrants to search the **Target Vehicle** described in Attachment A-1 and the **Target Device** described in Attachment A-2 and seize the items described in Attachment B-1 and B-2. The seizure of these items will aid law enforcement in their investigation of the crimes of distribution of controlled substances, and conspiracy to do same (21 U.S.C. §§ 841, 846); and illegal use of a communication facility (21 U.S.C. § 843(b)).

45. I request that the Court order that required notice be delayed for 90 days, until June 23, 2023, because I believe that Schnell is not currently aware of the nature and extent of the investigation. Although Schnell or an associate will likely take back possession of the vehicle after the search is completed and learn that the vehicle has been searched, he will not be aware that his electronic devices were searched. Disclosure of the scope of the warrants at this time would

compromise the ongoing investigation and could lead to harm to witnesses, destruction of evidence, or flight from prosecution.

/s/ Ryan S. Burke
Ryan S. Burke, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Mar 23, 2023**
Time: **9:03 PM, Mar 23, 2023**

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2

Description of Equipment to Be Searched

The equipment to be searched consists of the following ("**Target Device**"):

Black iPhone in a tie-dye case which was seized from Matthew Schnell on March 22, 2023 in Concord, New Hampshire.

This warrant authorizes the forensic examination of the **Target Device** for the purpose of identifying the electronically stored information described in Attachment B-2.

ATTACHMENT B-2

Description of Information or Items to Be Seized

I. All records on the **Target Device** described in Attachment A-2, in whatever form, that constitute evidence of violations of distribution of controlled substances, and conspiracy to do same (21 U.S.C. §§ 841, 846); and illegal use of a communication facility (21 U.S.C. § 843(b)) involving Matthew Schnell, Thomas Conway, Michael Raiche, and other co-conspirators including but not limited to:

a. Evidence of who used, owned, or controlled the equipment;

b. Evidence of the user's past whereabouts;

c. The identities and aliases of individuals who participated in the violations listed above;

d. Lists of associates and related identifying information;

e. Content associated with the above violations;

f. All bank records, checks, credit card bills, account information, and other financial records;

g. The locations where evidence, fruits, instrumentalities, or other items related to the violations listed above were obtained, is stored, or has been discarded;

h. The methods of communication between individuals engaged in the violations listed above, including the telephone numbers, messaging applications, and social media accounts used by the individuals;

i. The substance of communications regarding the planning, execution, transactions, and/or discussions of the violations listed above;

j. The substance of communications regarding the acquisition or disposal of items involved in the violations listed above;

k. The substance of communications regarding controlled substances, money, vehicles, communications devices, or other items acquired during or for activity that would result in the violations listed above;

l. Photographs of items or information related to the violations listed above;

m. The relationship between the users of the equipment and other co-

conspirators;

n. The identity, location, and travel of users of the **Target Device** and any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the violations listed above;

o. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

p. Evidence of the attachment of other hardware or storage media;

q. Evidence of counter-forensic programs and associated data that are designed to eliminate data;

r. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

s. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media; and

t. Records relating to the ownership, occupancy, or use of the location from which the equipment was obtained by law enforcement investigators.

II. Evidence of user attribution showing who used or owned the **Target Device** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

III. Serial numbers and any electronic identifiers that serve to identify the equipment.

DEFINITIONS

For the purpose of this warrant:

a. "Equipment" means any hardware, software, storage media, and data.

b. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

c. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

d. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

e. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

f. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner,

within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.